Opening Statement of the Honorable Cliff Stearns
Subcommittee on Oversight and Investigations
Hearing on "IT Supply Chain Security: Review of Government and Industry Efforts"
March 27, 2012
(*As prepared for delivery*)

With the growing reliance on the global economy for our goods and services, we are faced with the challenge that ensuring the security of those items has become ever more difficult. As the global economy grows, so does the complexity of the global supply chain. The U.S. Government is increasingly reliant on commercially available products for information technology (IT) services and components. This reliance forces the U.S. Government to depend on the trustworthiness of the global commercial supply chain.

Cyber or state-sponsored actors are capable of secretly inserting malicious code into both hardware and software during the manufacture of those items. For example:

- In July 2010, Dell announced that some of its PowerEdge motherboards contained malicious spyware that gathered information about a victim's Internet browsing habits and collected personally identifiable information.

- During a security conference in May 2010, IBM gave complimentary USB drives to attendees that contained two kinds of malware, including a keylogger program.

- In March of 2010, Spanish Cell Phone company, Vodafone, released a new version of a popular smartphone infected with a version of the Butterfly botnet, in addition to other malicious software.

These and many, many other instances of supply chain poisoning are capable of causing damage to, allowing a cyber criminal unauthorized access to, or allowing the exfiltration of sensitive or personally identifiable information from a victim's computer system.

Late last week, the Government Accountability Office released a report examining the risk and threats to the supply chains of both commercial and federal IT systems. The GAO studied four agencies involved in national security — the Departments of Defense, Energy, Homeland Security, and Justice — and their ability to assess the risk to their own IT supply chains and the steps they have taken to mitigate them. We are joined by the GAO today to discuss their findings and recommendations.

While DOD, DOE, DHS, and Justice each participate in interagency efforts to address supply chain security, some of these agencies have made more progress than others in addressing IT supply chain security risks. In particular, I was troubled to find that the GAO concluded that the Department of Energy had not developed clear policies that define what security measures are needed to protect against supply chain threats. Clearly defined security measures with comprehensive implementing procedures are necessary and vital to the protection of federal IT. One additional comment about the report as a whole is that there appears to be no

integrated response amongst the federal IT enterprise to address supply chain risks. Agencies are left to their own devices to address this risky and complex threat. I find this troubling.

Today, we will hear testimony from two panels of witnesses. On our first panel, we are joined by Mr. Gregory Wilshusen, Director of Information Security Issues at GAO and his staff who assisted in drafting the report. We are also joined by representatives of two agencies who are the subjects of the report. Mr. Mitchell Komaroff, Director of the Trusted Mission Systems Networks at the Department of Defense and Mr. Gil Vega, Associate CIO for Cybersecurity & Chief Information Security Officer at the Department of Energy. I look forward to their testimony, and getting a better understanding of the work they do to ensure the integrity of their agencies' IT supply chain.

I also want to welcome our second panel of witnesses who will provide us with an overview of the private sector approach to identifying IT supply chain risks and using industry best practices to mitigate them. We are joined by Mr. Larry Castro, Managing Director at The Chertoff Group and former National Security Agency/Central Security Service Representative to the US Department of Homeland Security (DHS). Also joining us is Dave Lounsbury, Chief Technology Officer at The Open Group an international IT standards board. Welcome to all of you.

As I mentioned previously, this is the subcommittee's third hearing in this Congress on cybersecurity. The purpose of this hearing, in particular, is to understand the threats and vulnerabilities to federal IT supply chains and how best to ensure their integrity. I have enjoyed working with Ranking Member DeGette and the Minority in these matters and look forward to our continued cooperation on cybersecurity issues.

###